REMARKS

The Office Action dated April 4, 2007 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-3, 5, 7-11, 14-16, 18, 19, 21, 22, 24-29, 31, 33, 35, 36, 38, 40, 43, and 46-48 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Support for the amendments may be found at least in paragraphs 0052, 0056, 0057, 0064, and 0070 of the specification. No new matter has been added. Claims 44 and 45 have been canceled without prejudice or disclaimer. Thus, claims 1-43 and 46-48 are currently pending in the application and are respectfully submitted for consideration.

Claims 1-11, 14-17, 19, 20, 22-29, 31, 33-35, 38, 39, and 43-48 were rejected under 35 U.S.C. §102(a) as being anticipated by Jennings (Extensions to the Session Initiation Protocol for Asserted Identity within Trusted Networks, SIP WG, Internet Draft). The rejection is respectfully traversed for at least the following reasons.

Claim 1, upon which claims 2-13 are dependent, recites a security server for use in a telecommunications network. The security server is configured to receive a message, to determine whether the message has been through a security check, and to forward the message within the telecommunications network regardless of the result of the determination, but if the result of the determination is that the message has not been

through a security check modify the message so as to indicate that the message has not been through a security check.

Claim 14, upon which claims 15-21 are dependent, recites a network processing element for use in a telecommunications network. The network processing element is configured to receive a message from another network element, to determine whether the message has been modified to indicate that it has not been through a security check and, if it has been so modified, to perform one or more security checks in respect of the message.

Claim 22, upon which claims 23 and 24 are dependent, recites a telecommunications network comprising a security server, and a network processing element. The security server is configured to receive a message, to determine whether the message has been through a security check, and, if the result of the determination is that the message has not been through a security check, to modify the message so as to indicate that the message has not been through a security check. The security server is also configured to forward the message to the network processing element regardless of the result of the determination.

Claim 25 recites a method of performing a security check on a message in a telecommunications network. The method includes receiving a message that has not been through a security check, determining that the message has not been through a security check, modifying the message so as to indicate that the message has not been

through a security check, and forwarding the message within the telecommunications network.

Claim 26, upon which claims 27-32 are dependent, recites a security server for use in a telecommunications network. The security server is configured to receive a message, to determine whether the message has been through a security check, and to forward the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check.

Claim 33, upon which claims 34-42 are dependent, recites a telecommunications network comprising a security server, and a network processing element. The security server is configured to receive a message, to determine whether the message has been through a security check, and to forward the message to the network processing element regardless of the result of the determination, but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check.

Claim 43 recites a method of performing a security check on a message in a telecommunications network. The method includes receiving a message that has not been through a security check, determining that the message has not been through a security check, and forwarding the message within the communications network in a manner that indicates that the message has not been through a security check.

Claim 46 recites a security server for use in a telecommunications network. The security server includes receiving means for receiving a message, determining means for determining whether the has been through a security check, modifying means for, if the message is determined not to have been through a security check, modifying the message to indicate that it has not been through a security check, and forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

Claim 47 recites a network processing element for use in a telecommunications network. The network processing element includes receiving means for receiving a message from another network element, and determining means for determining whether the message has been modified to indicate it has not been through a security check and, if it has been so modified, performing one or more security checks in respect of the message.

Claim 48 recites a security server for use in a telecommunications network. The security server includes receiving means for receiving a message, determining means for determining whether the message has been through a security check, and forwarding means for forwarding the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forwarding the message in a manner that indicates that the message has not been through a security check.

As will be discussed below, Jennings fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above.

Jennings discloses private extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems. Application of existing privacy mechanisms to the identity problem is also disclosed. The use of the extensions is only applicable in an administrative domain with previously agreed upon policies for generation, transport and usage of such information.

Applicants respectfully submit that Jennings fails to disclose or suggest all of the elements of the present claims. For example, Jennings does not disclose or suggest "modifying the message so as to indicate that the message has not been through a security check," as recited in claim 25 and similarly recited in claims 1, 22, and 46. In addition, Jennings fails to disclose or suggest forwarding "the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check," as recited in claim 26 and similarly recited in claims 33, 43, and 48. Jennings also does not disclose or suggest "determine whether the message has been modified to indicate that it has not been through a security check and, if it has been so modified, perform one or more security checks in respect of the message," as recited in claims 14 and 47.

Jennings only discloses a proxy which may receive messages from a node that it trusts, or from a node that it does not trust. When the proxy receives a message from a

node it does not trust, the proxy must authenticate the originator of the message and insert an appropriate P-Asserted-Identity header field into the message. If the proxy receives a message from a node that it trusts, then it can use the information in the P-Asserted-Identity header field as if it had authenticated the user itself. The messages are generally forwarded with a P-Asserted-Identity header regardless of whether the message was received at the proxy from a trusted node or an untrusted node (see Jennings, section 5). However, Jennings fails to disclose or suggest that, for a message that is determined to have not been through a security check, modifying the message so as to indicate that it has not been through a security check or otherwise forwarding it within the network in a way that indicates that the message has not been through a security check.

Accordingly, Jennings fails to disclose "modifying the message so as to indicate that the message has not been through a security check," as recited in claim 25 and similarly recited in claims 1, 22, and 46, or forwarding "the message within the communications network regardless of the result of the determination but, if the result of the determination is that the message has not been through a security check, forward the message in a manner that indicates that the message has not been through a security check," as recited in claim 26 and similarly recited in claims 33, 43, and 48. Similarly, Jennings does not disclose or suggest "determine whether the message has been modified to indicate that it has not been through a security check and, if it has been so modified, perform one or more security checks in respect of the message," as recited in claims 14

and 47. Therefore, Applicants respectfully request that the rejection of claims 1, 14, 22, 25, 26, 33, 43, and 46-48 be withdrawn.

Claims 2-13, 15-21, 23, 24, 27-32, and 34-42 are dependent upon claims 1, 14, 22, 26, and 33, respectively. Thus, claims 2-13, 15-21, 23, 24, 27-32, and 34-42 should be allowed for at least their dependence upon claims 1, 14, 22, 26, and 33, and for the specific limitations recited therein.

Claims 12, 30, 37, and 41 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Arkko (U.S. Patent Pub. No. 2002/0052200). The rejection is respectfully traversed for at least the following reasons.

Jennings is discussed above. Arkko discloses secured mobile application part (MAP) messages for telecommunication networks. An encrypted/authenticated MAP protocol message is sent between a first network element of a first telecommunications network and a second network element of a second telecommunications network. The first network element uses a master security association to derive a connection-specific security association, and includes in the encrypted/authenticated MAP message a parameter obtained from the connection-specific security association. Upon receipt at the second network element, the master security association is used to derive a connection-specific security association for use by the second network element. The second network element uses the connection-specific security association to decrypt/decode the MAP message.

Claims 12, 30, 37, and 41 are dependent upon claims 1, 26, and 33, respectively. As discussed above, Jennings fails to disclose or suggest all of the elements of claims 1, 26, and 33. Additionally, Arkko does not cure the deficiencies in Jennings with respect to claims 1, 26, and 33. Thus, the combination of Jennings and Arkko does not disclose or suggest all of the elements of claims 12, 30, 37, and 41. Furthermore, claims 12, 30, 37, and 41 should be allowed for at least their dependence upon claims 1, 26, and 33, and for the specific limitations recited therein.

Claims 13, 21, 32, and 42 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Soininen (Transition Scenarios for 3GPP Networks, Internet Draft). The rejection is respectfully traversed for at least the following reasons.

Jennings is discussed above. Soininen discloses an IP multimedia core network subsystem (IMS), which is a SIP based multimedia service architecture. The IMS includes a set of SIP proxies, servers, and registrars. Media Gateways offer connections to non-IP networks such as the PSTN.

Claims 13, 21, 32, and 42 are dependent upon claims 1, 14, 26, and 33, respectively. As discussed above, Jennings fails to disclose or suggest all of the elements of claims 1, 14, 26, and 33. Additionally, Soininen does not cure the deficiencies in Jennings with respect to claims 1, 14, 26, and 33. Thus, the combination of Jennings and Soininen does not disclose or suggest all of the elements of claims 13, 21, 32, and 42.

Furthermore, claims 13, 21, 32, and 42 should be allowed for at least their dependence upon claims 1, 14, 26, and 33, and for the specific limitations recited therein.

Claims 18, 19, and 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Peterson (A Privacy Mechanism for the Session Initiation Protocol, Network Working Group, Internet Draft). The rejection is respectfully traversed for at least the following reasons.

Jennings is discussed above. Peterson discloses mechanisms for the Session Initiation Protocol (SIP) in support of privacy. Guidelines are provided for the creation of messages that do not divulge personal identity information.

Claims 18, 19, and 20 are dependent upon claim 14. As discussed above, Jennings fails to disclose or suggest all of the elements of claim 14. Additionally, Peterson does not cure the deficiencies in Jennings with respect to claim 14. Thus, the combination of Jennings and Peterson does not disclose or suggest all of the elements of claims 18, 19, and 20. Furthermore, claims 18, 19, and 20 should be allowed for at least their dependence upon claim 14, and for the specific limitations recited therein.

Claims 36 and 40 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Haukka (U.S. Patent Pub. No. 2003/0210678). The rejection is respectfully traversed for at least the following reasons.

Jennings is discussed above. Haukka discloses a method and apparatus for connecting terminal equipment to a wireless network with a mobile terminal, wherein the mobile terminal is assigned proxy functions that control access of the terminal equipment

to an internet protocol multimedia subsystem (IMS) in the wireless network. The proxy control functions include identification or authentication functions, as well as call control functions. The terminal equipment performs protocol stream processing functions for communicating with the internet protocol multimedia subsystem (IMS).

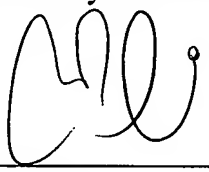
Claims 36 and 40 are dependent upon claim 33. As discussed above, Jennings fails to disclose or suggest all of the elements of claim 33. Additionally, Haukka does not cure the deficiencies in Jennings with respect to claim 33. Thus, the combination of Jennings and Haukka does not disclose or suggest all of the elements of claims 36 and 40. Furthermore, claims 36 and 40 should be allowed for at least their dependence upon claim 33, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art fails to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-43 and 46-48 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf